Support for Multiple Hash Algorithms in Cryptographically Generated Addresses (CGAs)

INT area meeting

IETF66 - Montreal

Marcelo Bagnulo - Jari Arkko

Motivation

- Recent attacks against the collision-free property of hash functions (SHA1)
- Hoffman & Schneier, RFC 4270
- Bellovin & Rescorla, "Deploying a new hash algorithm”
- First step: analyze the impact of such attacks in current protocols
- Second step: provide hash function migration support

Impact of collision attacks in CGAs

- Recent attacks allow obtaining two messages M1 and M2 that have the same hash value with much less than 2^(L/2) attempts.
- Such attacks challenge the application of such hash function for the provision of non-repudiation capabilities.

Currently proposed usages of CGAs

- SeND
- shim6
- OMIPv6
- Prove “ownership” of address
- No no-repudiation provided
- Recent attack do not affect current usages of CGAs

Multiple Hash Algorithm Support in CGAs

- SHA1 hard-coded in current CGA generation procedure
- Current applications are not affect by collision attacks, reasons for hash function agility support:
  - Future applications may require it
  - Possible evolution of attacks

Where to encode the hash function?

- Must be encoded in the address itself to prevent downgrading attacks
- Using more iid bits woudl result in weaker CGAs
- Proposal: use the Sec field to encode both current Sec information and the hash function used
  - Reserve 3 values as currently defined

IANA considerations new registry CGA SEC

- Initial assignments

Name	Value	RFC
SHA-1_0hash2bits	000	3972
SHA-1_16hash2bits	001	3972
SHA-1_32hash2bits	010	3972